

ABSTRACT OF THE DISCLOSURE
STORING KEYS IN A TCPA CRYPTOLOGY DEVICE

A method and system for managing cryptology keys in a TCPA subsystem such as a Trusted Platform Module (TPM). The TPM encrypts/decrypts data being communicated with a processing system. Internal to the TPM is limited memory for storing cryptology private keys used in the encryption/decryption. Under the TCPA specification, the keys are hierarchical, such that a parent key must be in the TPM to load into the TPM the requested child cryptology private key. Thus there is an expense associated with replacing an existing key. This expense is determined by the probability that the evicted key will be needed and thus re-stored in the future and the likelihood that ancestor keys will have to be loaded into the TPM in order to load the requested child key. The present invention presents a method for determining this expense, in order to determine which key should be evicted.

5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995